



NIT-307

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

Appl. No.: 09/977,351 Confirmation No. 3978  
Applicant: Y. IKEDA  
Filed: October 16, 2001  
Title: INFORMATIONDISTRIBUTING SYSTEM AND METHOD  
THEREOF  
TC/AU: 2134  
Examiner: T. Ho  
Customer No.: 24956

**SUBMISSION OF CERTIFIED PRIORITY DOCUMENT**

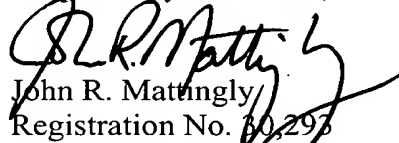
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Sir:

Applicants submit herewith a certified priority document of corresponding Japanese Patent Application No. 2000-316200, filed October 17, 2000 for the purpose of claiming foreign priority under 35 U.S.C. § 119.

Applicants respectfully request that the priority document be submitted and filed and officially considered of record.

Respectfully submitted,

  
John R. Mattingly  
Registration No. 30,293  
Attorney for Applicant

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.  
1800 Diagonal Road, Suite 370  
Alexandria, Virginia 22314  
(703) 684-1120  
Date: October 31, 2005

BEST AVAILABLE COPY

CERTIFIED COPY OF  
PRIORITY DOCUMENT

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2000年10月17日

出 願 番 号

Application Number:

特願2000-316200

出 願 人

Applicant(s):

株式会社日立製作所

09/977,351

NIT-307

Mattigly Stanger Malur

703 684-1120

2001年10月19日

特 許 庁 長 官  
Commissioner,  
Japan Patent Office

及 川 耕 造

【書類名】 特許願

【整理番号】 NT00P0535

【提出日】 平成12年10月17日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 15/16

【発明者】

【住所又は居所】 神奈川県秦野市堀山下1番地 株式会社日立製作所 エ  
ンタープライズサーバ事業部内

【氏名】 池田 圭伸

【特許出願人】

【識別番号】 000005108

【氏名又は名称】 株式会社日立製作所

【代理人】

【識別番号】 100068504

【弁理士】

【氏名又は名称】 小川 勝男

【電話番号】 03-3661-0071

【選任した代理人】

【識別番号】 100086656

【弁理士】

【氏名又は名称】 田中 恭助

【電話番号】 03-3661-0071

【選任した代理人】

【識別番号】 100094352

【弁理士】

【氏名又は名称】 佐々木 孝

【電話番号】 03-3661-0071

【手数料の表示】

【予納台帳番号】 081423

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報提供装置および方法

【特許請求の範囲】

【請求項 1】

Webサーバと、インターネットに接続され前記Webサーバの配信する情報の複製を保持しユーザからの要求に応じて前記情報の配信を行なう複製Webサーバと、前記Webサーバと前記複製Webサーバの間に設置されあらかじめ定められたプロトコルを用いたもので且つ、前記複製Webサーバからの接続要求であるときのみ接続を許可するファイアウォールとを備えたことを特徴とする情報提供装置。

【請求項 2】

前記Webサーバは前記ファイアウォールを通した接続要求が許可された接続相手からのものかどうか判断し、そうでなければ通信を切断し、そうであれば要求されたデータを前記ファイアウォールを通して接続要求を出した前記複製Webサーバへ送信することを特徴とする請求項 1 記載の情報提供装置。

【請求項 3】

Webサーバと、インターネットに接続され前記Webサーバの配信する情報の複製を保持し、ユーザからの要求にしたがって保持する情報を提供する複数の複製Webサーバと、前記Webサーバと前記複数の複製Webサーバの間に設けられたファイアウォールとを有し、前記複数の複製Webサーバは互いに保持する情報が一致しているかどうかを判定することを特徴とする情報提供装置。

【請求項 4】

前記互いに保持する情報が一致しているかどうかの判定はそれぞれの保持する情報の検査コードを比較することにより行なわれることを特徴とする請求項 3 記載の情報提供装置。

【請求項 5】

更に、複数の前記複製Webサーバへのユーザ端末からの接続要求を前記複数の複製Webサーバに分散せしめる負荷分散装置を備えたことを特徴とする請求項 3 記載の情報提供装置。

## 【請求項 6】

Webサーバと、インターネットに接続され前記Webサーバの配信する情報の複製を保持し、ユーザからの要求にしたがって保持する情報を提供する複数の複製Webサーバと、前記Webサーバと前記複数のWebサーバとの間で通信を行なわせる専用接続線を備えたことを特徴とする情報提供装置。

## 【請求項 7】

配信される情報を記憶する情報処理装置と、インターネットに接続され配信される情報の複製を記憶し、要求に従い情報の複製を配信する複数の情報配信装置とを有する情報提供装置における方法であって、前記情報処理装置が保持する情報の一部又は全てを前記情報配信装置の一つ又は複数に転送するステップと、複数の前記情報配信装置が保持する情報を互いに比較するステップとを有することを特徴とする情報提供方法。

## 【請求項 8】

配信される情報を記憶する情報処理装置と、インターネットに接続され配信される情報の複製を記憶する複数の複製Webサーバとを有する情報提供装置における方法であって、ある複製Webサーバから他の複製Webサーバの指定する情報の一致をチェックする場合において、他の複製Webサーバにおいて指定された情報があるかどうかを調べ、あるときはその情報の検査コードを前記あるWebサーバに転送し、前記あるWebサーバにおいて、前記指定された情報に対応する自サーバが記憶するファイルの情報の検査コードを求め、これら2つの検査コードを比較し、一致するときはチェックを終了し、一致しないときは前記情報処理装置から対応する情報を入手して保存することを特徴とする情報提供方法。

## 【請求項 9】

前記他のWebサーバにおいて指定された情報がないとき前記情報処理装置から当該情報を入手し保存すると共に検査コードを前記あるWebサーバに転送することを特徴とする請求項 8 記載の情報提供方法。

## 【請求項 10】

前記情報処理装置にも指定された情報がない場合に前記あるWebサーバの当該情報を削除することを特徴とする請求項 9 記載の情報提供方法。

【請求項 1 1】

配信される情報を記憶する情報処理装置と、インターネットに接続され配信される情報の複製を記憶し、要求に従い情報の複製を配信する複数の情報配信装置とを有する情報提供装置における方法であって、前記情報配信装置が配信する情報に付加された電子署名により、情報の正当性を評価することを特徴とする情報提供方法。

【請求項 1 2】

前記電子署名の有無、または電子署名の数により、前記情報配信装置が配信する情報の配信先の範囲を制御することを特徴とする請求項 1 1 記載の情報提供方法。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、インターネットに接続された情報処理システムに対し、システム内外からの不正な改ざんからシステムに登録されている情報を防護する方法および防護を施した装置に関する。

【0 0 0 2】

【従来の技術】

近年インターネットの普及により、多くの相互接続されたコンピュータ機器が様々な用途で利用されている。このようなコンピュータ機器に対し不正なアクセスからシステムを防護する手段として、次のような方式が実用化されている。図 1 は最も代表的な防護例である。ファイアウォール（防火壁）と呼ばれるシステムをインターネットと情報処理システムの途中に接続し、ここで不正なアクセスの振るい落としをすることによってインターネット側に対して提供するサービスを制限している。また、図 2 のようにサービスを提供するコンピュータ機器をファイアウォールの外側に置き、コンピュータ機器側で何らかの防護策を取る場合もある。

【0 0 0 3】

特開平 1 1 - 2 6 6 2 7 9 号公報の記載では、図 2 に示すシステムのようにフ

ファイアウォールの外部にメールサーバを設置することで、ファイアウォール外部のユーザがファイアウォールを介さずにメールの送受信を行うことを可能とし、ファイアウォール内のネットワークのセキュリティを高めている。

【0004】

【発明が解決しようとする課題】

従来の防護システムは、ファイアウォールと呼ばれるシステムに頼った形となり、外からの攻撃に対する強さはファイアウォールの強さに依存してしまう問題があった。また、ファイアウォールは一般に高価な導入コストと管理コストを必要とする。

【0005】

また、インターネットに対して様々なサービスを提供するにあたって、それに応じた情報処理システムに対する様々な機能追加が必要になるが、これらの機能追加によりファイアウォールの内部構造は複雑化してしまい、性能の劣化や新たなセキュリティホールを産み出す要因になってしまう。

【0006】

更に、サービス提供機器をファイアウォールの外側に置いた場合、攻撃に対する防御の必要性からサービスを提供する機器に対してファイアウォールの内側から容易に入ることができない。

【0007】

また、一般的なファイアウォールでは外部からの攻撃には耐えられるが、内部からの不正な改ざんに対しては配慮がなされておらず、効力を持たない。

【0008】

従来のシステムでは情報処理システムの情報に不正な改ざんがあった場合に対して発見が容易でなく、不正な侵入への常時監視に対し高い費用が発生する。

【0009】

従来のプロキシサーバは、外部インターネットへの代理接続（WWW閲覧ソフトを実行しているユーザのコンピュータの代理としてユーザの要求するWWWサーバに接続を試み、そして、接続が成功した場合、そのWWWサーバから取得できたデータをユーザに送信すること）や一次保存（WWWサーバから取得できたデ



ータをユーザに送信するとともに、同一データの要求に備えて自らの記憶領域に一時的に保存すること）を目的とするものであり、外部向けサービス提供機器を保護する用途として内部インターネットへの接続を代行するものではない。また、従来のミラーサーバは、ミラー対象サーバの内容を複写し、システム及びネットワーク的な負荷分散を目的とし、防護システムに対する特別な配慮はない。これらのように、従来のミラーサーバやプロキシサーバの場合、セキュリティに於ける配慮は従来の防護システムと何ら変わらず、本質的に解決されない。

#### 【 0 0 1 0 】

本発明の目的は、インターネットに対してサービスを提供する機器に対し、不正な改ざんに強く監視が容易なシステムを提供し、システムの運用コストを低減することである。

#### 【 0 0 1 1 】

##### 【課題を解決するための手段】

上記目的を達成するため本発明では、ファイアウォールの内側にあるサービス提供システムのレプリカ（複製）をファイアウォールの外側に複数置き、利用者はこれらレプリカからのみサービスの提供を受けるようにする。サービス提供者はファイアウォールの内側にある本来のサービス提供システムに対し、情報を登録する。このシステムはファイアウォールの内側であるので、セキュリティホールをあまり気にせずに様々な手段で情報を登録することができる。

#### 【 0 0 1 2 】

複数のレプリカは本来のサービス提供システムの情報を常に複写しておくようにする。レプリカは定期的にレプリカ同士が保持する情報の内容を互いに比較することにより、不正な改ざんが発生したかどうかのチェックを行う。ここでレプリカの保持する情報の間に差異がある場合はファイアウォールの内側にある本来のサービス提供システムから本来あるべきデータがレプリカに対し複写され、レプリカによって不正な改ざんがあったかどうかを検査し、元の情報に修正し、管理者に通報することができる。

#### 【 0 0 1 3 】

レプリカに複写される情報には電子署名を付加することができる。この機能を

使用する場合、レプリカは利用者に情報を発信するにあたって電子署名が有効であるかどうかを検査し、有効である場合は発信し、無効である場合は管理者に連絡する（レプリカがWWWサーバに無効であることを連絡の後、WWWサーバが管理者にメールやSNMPメッセージ等で連絡する）。これにより、必要な電子署名を付加する権限のない者が情報の公開や改変行為を行うことをできなくすることができる。

## 【 0 0 1 4 】

複数のレプリカは互いにサービスを行なうサーバとして入れ替わることにより、インターネット側からは同一の機器に見せる。このことにより、内部的に不正な接続のあった装置とそうでない装置を分け、それらを互いに比較しあうことができる。また、サービスを提供するレプリカの負荷を分散し、速度の低下を防ぐことができる。

## 【 0 0 1 5 】

## 【発明の実施の形態】

図3は本発明を、WWWサービスを提供するシステムの実施の形態としてブロック図で示したものである。図3において、インターネット1から見えるレプリカ8は4台、WWWサーバ3は1台しか示されていないが、実際にはこれ以上の台数が接続されていたり、1台の機械を論理的に複数台に見立てている場合も考えられる。また、このレプリカ8は多段に接続することもできる。さらに、このレプリカ8はインターネット上の他の場所にあっても良く、レプリカ8の配置次第ではネットワークの負荷分散をすることができる。

## 【 0 0 1 6 】

登録情報作成者は登録情報作成システム4からWWWサーバ3に情報を登録する。WWWサーバ3はファイアウォール2で防護されている為、この時用いられる手段は、一般に用いられるネットワーク転送手順の何れでも良い。これは、例えばWWWサーバ3をファイルサーバに見立て、WWWサーバ3とPCなどで構成される登録情報作成システム4間でファイル共有を行うことで実現できる。

## 【 0 0 1 7 】

図10を用いてレプリカ8、ファイアウォール2、WWWサーバ3の間の通信

について説明する。レプリカ 8 はファイアウォール 2 を介して WWW サーバ 3 と通信を行うが、この際ファイアウォール 2 は HTTP 用のポートのみを外部ネットワークに対し開放している。もし外部ネットワークからの通信が、HTTP 以外のポートに対するものであれば (1 0 0 1 No)、ファイアウォール 2 はこの通信を切断する。外部ネットワークからの通信が HTTP 用のポートに対するものであるなら (1 0 0 1 Yes)、ファイアウォールは次にこの通信の発信元を、パケットのヘッダ中の情報から識別し、レプリカ 8 からの接続要求かを判断する (1 0 0 2)。パケットの発信元が外部ネットワークに設置されたレプリカ 8 であれば接続を許可するが、それ以外の機器が発信元である場合は、通信を切断する。もし HTTP により接続要求をしている機器がレプリカ 8 であるなら、ファイアウォール 2 はレプリカ 8 に対し接続を許可し、接続許可の応答をファイアウォール 2 より受けたレプリカ 8 はコマンドの作成 (1 0 0 3) 及び送信を行い、WWW サーバ 3 に対し処理を要求する。レプリカ 8 からのコマンドを WWW サーバ 3 に仲介するファイアウォール 2 では、コマンドの文法チェックを行い (1 0 0 4)、文法に誤りがある場合には通信を切断する。チェックの結果文法が正しい場合は、ファイアウォール 2 は WWW サーバ 3 に対し HTTP による接続要求を行う。WWW サーバ 3 は、接続要求の発信元を識別し (1 0 0 5)、それが許可された機器であれば接続許可の応答を返信するが、そうでなければ通信の切断を行う。接続許可の応答を受けたファイアウォール 2 は、レプリカ 8 から送信されたコマンドを WWW サーバ 3 へ送信する。ファイアウォール 2 からのコマンドを受けた WWW サーバ 3 は、コマンドにより要求された処理に応じてデータを作成し (1 0 0 6)、このデータをファイアウォール 2 に送信する。ファイアウォール 2 はこのデータをレプリカ 8 に送信し、さらにレプリカ 8 に対して新たなコマンドの受け付けを行う。引き続きレプリカ 8 が WWW サーバ 3 に処理を要求するなら (1 0 0 7 No)、レプリカ 8 におけるコマンド作成以後の処理を繰り返すが、WWW サーバ 3 に対する要求が無いのであれば、レプリカ 8 はファイアウォール 2 に対し通信を切断する要求を送信し、ファイアウォール 2 からは WWW サーバ 3 に対し同様に通信を切断する要求を送信することでレプリカ 8、ファイアウォール 2、WWW サーバ 3 の間の通信を切断して一連の処理を終了す

る。

【0018】

上記のようにファイアウォールはレプリカからのHTTPを用いた接続要求のみを受け付けるため、市販の高価なファイアウォールシステムを用いなくとも、HTTPプロキシ（代理）サーバをフリーソフトウェアを用いて安価に構築し、ファイアウォールとして利用することも可能である。

【0019】

勿論、顧客が既に導入しているファイアウォールやWWWサーバをそのまま利用することも可能であり、この場合顧客はレプリカ8を新規導入し、WWWサーバ上に追加の設定（レプリカの複写、更新の機能の追加）を実施してWWWサーバ3とする。レプリカ8はこれらの機構を通して、WWWサーバ3の複製となる。このように一般的なHTTP接続のみを用いてレプリカ8はWWWサーバ3の複製となるので、レプリカ8はWWWサーバ3の内容を書き換えることが出来ない。

【0020】

レプリカ8はインターネット1上のユーザ端末に対し、所定のポートに対する接続及び通信のみを許可する。このとき、この接続を待つ以外のポートは使用せず、ユーザ端末が接続できないようにする。ネームサーバ9は登録されているエントリを随時変更し、同一のレプリカにアクセスが集中しないようにする。例えば図11に示すように、ユーザ端末がwww.japan.co.jpのドメインネームを持つWWWサーバへの接続要求を行うと、ネームサーバはこのWWWサーバの複製であるレプリカに与えられたIPアドレス（1）～（4）のうちの1つを、ラウンドロビン方式で、もしくはランダムに返信する。ユーザはこのネームサーバが返信したIPアドレスに対し接続を行うため、図11に示す4つのレプリカの間でユーザからのアクセスが分散されるために1つのレプリカに対しアクセスが集中することを回避することができる。

【0021】

これは図5のようにスイッチ10を用い、レプリカ8への通信経路を切り替えることで実現することもできる。レプリカ8とファイアウォール2を、図4や図

5のようにインターネット1とは別のネットワークを経由して接続し、ファイアウォール2をインターネット1からネットワーク的に分離すれば、システムとしての防護性能を更に上げることができる。以上のことからネームサーバ9やスイッチ10は負荷分散装置として機能する。

#### 【0022】

また図6のように、レプリカ8及びスイッチ10を1つの機器であるWWWセキュリティ装置11として構築し、専用ケーブル等の一般的なネットワーク以外の手段を用いWWWサーバ3と直接接続することで、防護性能を保ったままファイアウォール2を省略することもできる。WWWセキュリティ装置11はインターネット1からの接続要求をスイッチ10で分散し、複数のレプリカ8に分配する。このレプリカ8は論理的に複数台とする構成でも良いし、スイッチ10を使わず図3や図11で説明したようなネームサーバを用いて振り分けても良い。

#### 【0023】

レプリカ8はインターネット1上に存在するユーザ端末からの接続要求を所定のポートで受けると、自らが保持しているWWWサーバ3の情報の複製をユーザ端末に送信する。図9を用いて、レプリカ8が、ユーザ端末が要求する情報を配信する処理を説明する。

#### 【0024】

ユーザ端末はGETコマンドを用いて／h o g e／i n d e x．h t m lというファイルをレプリカ8に要求するが、レプリカ8がこのファイルの複製を保持している場合は（901 有）、WWWサーバ3に対しアクセスは行わない。レプリカ8が保持するファイルに後述する電子署名が付加されている場合はその電子署名のチェックを行い（903）、電子署名が適正なものであれば（903 OK）ユーザに／h o g e／i n d e x．h t m lファイルを送信し、電子署名に誤りがあれば（903 NG）WWWサーバ3にエラーを通知しまたユーザに対しても該当するファイルが存在しない旨をエラー通知する。この電子署名のチェックはオプションであり、電子署名を用いない場合はこの処理を行わずにファイルをユーザ端末に送信する。レプリカ8が／h o g e／i n d e x．h t m lファイルを保持していない場合は（901 無）、図10に示した処理を経てレ

プリカ 8 と WWW サーバ 3 間で接続を確立した後、WWW サーバ 3 に対しコマンドを送信して / h o g e / i n d e x . h t m l ファイルの送信を要求する（新規複写）。WWW サーバ 3 はファイルを保持している場合（9 0 2 有）はレプリカ 8 にそのファイルを送信し、レプリカ 8 は送信されたファイルに電子署名が付加されていればそのチェックを行い、そしてファイルをユーザに送信する。WWW サーバ 3 がファイルを保持していない場合（9 0 2 無）は、WWW サーバ 3 からレプリカ 8 ならびにユーザ端末に対してエラーを通知する。

## 【 0 0 2 5 】

基本的には上述のように、新規複写はユーザの要求があったページがレプリカ 8 上に存在しない場合に WWW サーバ 3 からその情報を取得することにより行い、一方、WWW サーバ 3 が保持する最新の情報をレプリカ 8 が保持する同じ情報に反映する処理（更新）は、レプリカ 8 と WWW サーバ 3 とのコンペアチェックの結果によって行うことができる。これは、以下の手順で予め用意しておくこともできる。

## 【 0 0 2 6 】

図 9 の更新の場合、レプリカ 8 は WWW サーバ 3 もしくはカスケード接続された上位のレプリカ 8 に接続を行う（9 0 4）。そして該当の情報について CRC のエラーチェックコードの計算を行なう（9 0 5）。一方、WWW サーバ 3 では求められたファイルが存在するかどうかを判定し（9 0 2）、なければ（9 0 2

無）、エラー情報をレプリカ 8 へ送る。レプリカ 8 ではこれを受けて当該ファイルを削除する（9 0 7）。該当するファイルがあれば（9 0 6 有）、同様にその情報について CRC のエラーチェックコードを計算し、作成する（9 0 8）。これを更新日付と共にレプリカ 8 に転送する。次に、レプリカで計算され求められた CRC と WWW サーバから転送された CRC とを比較し一致するかどうか調べる（9 0 9）。一致すれば、情報の更新はなかったことを意味しレプリカ 8 の情報の更新はしない（9 1 0）。一致しなければ、レプリカ 8 は WWW サーバにファイルの転送を要求し、これを保存する（9 1 1）。

## 【 0 0 2 7 】

以上の処理はインターネット上のユーザとのやり取りは遮断し、レプリカ 8 と W

WWサーバ3の間だけで実行される。

【0028】

即時更新のときは、レプリカ8はGETコマンドで更新情報の要求を出す(912)。WWWサーバ3は情報の更新が生じるまでこの要求を保留しておき、更新が発生した時点で更新情報を応答として返す。これを用いることにより、WWWサーバ3の更新後即時にレプリカ8を更新することができる。

【0029】

レプリカ8はWWWサーバ3の全てのコンテンツに対する複製を保持するのが基本であるが、設定により保持する複製の量や複製する場所を設定できる。すなわち、サーバ上のコンテンツが複数のディレクトリやファイルから構成される場合、どこからどこまでのディレクトリやファイルを複製の対象とするかを指定できる。さらに、複製の対象とするファイルの数やサイズに制限を設けるよう指定することができる。これによって、例えば、ディレクトリ毎に複製するファイルの数や全体サイズを制限したり、大きなファイルの複製制限等の制御ができる。また、複製する対象を容量やアクセス頻度等に応じて自動的に選択し、動的に変化させることができる。

【0030】

外部ネットワークに複数設置されたレプリカ8には、ネットワーク上のユーザによる不正な改ざん行為に対する防衛手段が施されていないため、レプリカ8同士や内部ネットワーク上のWWWサーバ3との間で定期的にコンペアチェックを行い不正な改ざんを発見し、レプリカ8が保持し配信する情報の信憑性を保つ。

【0031】

図8を用い、1台目のレプリカ8(装置A)が保持する／foo／index.htmlファイルのコンペアチェックの処理を説明する。まず、装置Aは2台目のレプリカ8(装置B)に対し、HTTPプロトコルの“HEAD /foo／index.html”コマンドにより、装置Bが保持する／foo／index.htmlファイルの属性情報の送信を要求しコンペアチェックを開始する(801)。装置Bでは当該ファイルがあるかを調べ(802)、有る場合には当該ファイルのCRC計算を行なう(803)。そしてそれを更新日付と共に装

置Aに送る。一方、装置Aでも当該ファイルのCRC計算を行ない(804)、装置Bから転送されたCRCと一致するかどうか判定する(805)。一致すれば、不正な改ざんがなかったとしてチェック終了する(806)。

## 【0032】

また、装置AからHEADコマンドを受けた装置Bが要求されたファイルを保持していない場合(802 無)、装置BはHEADコマンドの応答を装置Aに返す前にWWWサーバ3にGETコマンドで接続しファイルの送信要求を行う。WWWサーバ3に当該ファイルがあれば(807 有)、当該ファイルを取得して保存し(808)、同様にCRC計算を行なう(809)。

## 【0033】

これは、装置AのCRCと比較され一致すればチェック終了し(806)、一致しなければ改ざんなどにより装置Aのファイルが正しくないとしてWWWサーバ3から取得したファイルを装置Aに保存する(810)。

## 【0034】

WWWサーバ3が要求されたファイルを保持していない場合そのファイルは、WWWサーバ3から削除されたか、ネットワーク上の侵入者により装置Aに対し勝手に追加されたファイルだと解釈される。そこで装置BはHEADコマンドの応答として装置Aに該当ファイルの削除命令を返し、WWWサーバ3には新たな属性を加えたHEADコマンドで削除命令発行の旨を通知する。装置Aは削除命令を受けた後、実際にそのファイルを削除し、削除完了の旨を新たな属性を加えたHEADコマンドでWWWサーバ3に通知する。これは、削除せず別の記憶領域に一時保管したり、POSTコマンドでWWWサーバ3の特定記憶領域に保管することもでき、これにより不正アクセスであった場合に証拠を残すことができる。これらの応答は互いに暗号を用いることもでき、ネットワーク的に遠隔なレプリカに対しても安全に削除情報を送ることができる。以上のようにコンペアチェックは実施されるが、レプリカ8とWWWサーバ3との間が独自手順で実装されている場合、HEAD、GET、POST各コマンドの仕様に縛られない、更に自由度のある設計をすることができる。

## 【0035】



そしてレプリカ 8 は必要に応じて他のファイルに対し同様にコンペアチェックを行う。

## 【 0 0 3 6 】

コンペアチェックはレプリカ 8 同士のみではなく、レプリカ 8 と WWW サーバ 3 との間で行うことも出来る。WWW サーバ 3 ではファイルの更新が行われる可能性があるため、WWW サーバ 3 を相手にコンペアチェックを行う場合は、レプリカ 8 が保持する情報が最新の内容であるか、情報の更新チェックを同時に行うことにもなる（図 9 における更新）。

## 【 0 0 3 7 】

HEAD コマンドには新たな属性を加え（ファイルの日付やサイズ等を返す機能に加え検査用コードも返すように機能拡張する）、ファイルの検査コード（チェックサムや CRC コード等）を得られるようにしておく。

## 【 0 0 3 8 】

HEAD コマンドで取得した他装置又は WWW サーバが持つ属性情報は、それを用いて比較を行うことが目的であるため、送受信するデータはハッシュ等により非可逆的に暗号化されていても良い。

## 【 0 0 3 9 】

WWW サーバ 3 に登録する情報は前述のように、登録時に署名生成手続きにより電子署名を行うことができる。電子署名を使用する場合の流れを図 1 2 に示す。レプリカ 8 において、GET コマンドによって要求されたファイルを準備する（1 2 0 1）。次に、電子署名があるかどうかを調べ（1 2 0 2）、ないときはこれはユーザには送信できないファイルと判断されるから、ユーザにはエラー、ファイル無しとの応答がなされる。署名があった時、この署名を評価する（1 2 0 3）。そして対象ユーザ毎に配信可のものか、配信否のものかを判断する（1 2 0 4）。送信可のユーザにはデータ送信をし、送信否のユーザにはエラー、ファイル無しとの応答がなされる。

## 【 0 0 4 0 】

図示していないが配信情報中の電子署名が正当な署名でない場合、レプリカ 8 は WWW サーバ 3 が保持する情報を再複製し、その署名を検査することもできる。

このとき、再複製の情報も正当でない場合、利用者にはエラーの旨を配信する。  
いずれの段階でも管理者に対し不正署名の旨を通報することができる。

## 【0041】

また、電子署名の利用により、図7のように配信情報をグループ分けし、配信先の制御を行うことができる。図7においては例として、情報に対しA、B、C、Dの4種の電子署名が付加され得る。ここで、4種全ての電子署名が付加された情報1は、社内および関連会社を含む社外にまで配信される情報として識別される。B、C、Dの3種の電子署名が付加された情報2は、社内および関連会社内までを情報配信の範囲として識別される。以下、情報3、情報4そして情報5と付加する電子署名の種類に応じてその情報の配信範囲を設定することが可能である。

## 【0042】

この処理を示したものが図13である。データの配信要求(1301)を受けたレプリカ8もしくはWEBサーバ3は、まずユーザのIPアドレスが社内もしくは社外どちらのものであるかを識別する(1302)。ユーザのIPアドレスが社内のものであった場合は、さらに同じ部署のものかを識別する(1303)。もし同じ部署のものであれば(ユーザC)、電子署名のチェックは行わずに情報の配信を行う(1304)。ユーザのIPアドレスが他部署のものであった場合(ユーザB)は、ファイルを準備すると共に(1305)、配信する情報に付加された電子署名が他部署に対する情報配信を許可する種類のものであるかをチェックし(1306)、許可するものであれば配信を行いそうでなければユーザにエラー通知を行う。ユーザのIPアドレスが社外のものであった場合(ユーザA)は、ファイルを準備すると共に(1308)、配信する情報に付加された電子署名が社外に対して配信することを許可する種類のものであるかをチェックし(1309)、そうであれば配信しそれ以外のものであればユーザにエラーを通知し、その情報の配信は行わない。

## 【0043】

以上のような電子署名の利用法は、従来社内向けと社外向け等のようにWWWサーバ3を用途別に分けていた場合に有効で、電子署名の違いや有無により、配

信先を分別することができる。例えば、電子署名が無い情報はレプリカ 8 には複製されないか、複製されても配信できないので、WWWサーバ 3 に直接アクセス可能な場所からのみアクセス可能となる。これにより、社外向け情報は電子署名付、社内向け情報は電子署名無しと区別することにより、配信情報を社外／社内向けというようにグループ分けができる。また、電子署名の評価にあたって、署名内に記された情報により、特定の顧客のみの配信等の制御をすることもできる。

## 【 0 0 4 4 】

レプリカ 8 は基本的に WWWサーバ 3 が配信する情報の複製作成機器であり、一度複製元の設定をしてしまえば大きな変更がない限りオペレータによる操作の必要はない。複製元の設定とはどの WWWサーバ 3 をどれだけ複製するか、検査コードを使用するか、電子署名や暗号を使用するか、即時更新するかどうかの複製のポリシーなどを指す。

## 【 0 0 4 5 】

ファイアウォール 2 は通過させた情報について発信元等の属性情報を累積するが、この累積された属性情報は WWWサーバ 3 で収集可能であるので、レプリカ 8 と同様に、オペレータによるファイアウォール 2 への操作の必要はない。このように、レプリカ 8 とファイアウォール 2 は運用される時点では人手を介した操作を必要としないので、このレプリカ 8 とファイアウォール 2 を物理的に隔離した部屋に置き、物理的な鍵をかけることができる。このことにより物理的な鍵を持たない、システム内部の者による不正なシステム侵入、情報公開や改変行為を防ぐことができる。

## 【 0 0 4 6 】

レプリカ 8 と WWWサーバ 3 の間は一般的なネットワーク手順で接続する必要は無いので、WWWサーバ 3 側に通信機構を増設し独自の通信手順で接続するようにすれば、インタネットプロトコルを使用しないので、ファイアウォール 2 の必要がなくなる。これはシステム全体のコストダウンに寄与することができ、ファイアウォール 2 上のセキュリティ欠陥が原因でのシステム不正侵入やシステムダウン等を防ぐことができる。この独自手順での接続は、図 6 のように装置 1 1

として実装しなくとも、図4や図5の構成で実施することも可能である。装置11は、レプリカ8とWWWサーバ3との通信に独自手順を使用しない場合、ファイアウォール2を内蔵してしまっても良い。また、装置11はルータ等、他のネットワーク装置の内蔵オプションとして実装しても良いし、WWWサーバ3に装置11を内蔵しても良い。これらのように装置として本発明のシステムを実装した場合、システム構築や管理が簡便になるという利点がある。

【0047】

以上、本発明の実施の形態を説明したが、レプリカ8を多段接続し、後段のレプリカ8は前段からの接続のみ受け付けるようにすれば、さらに防護性能を上げることができる。この場合、前段となるレプリカ8はインターネット1上の他の場所にあっても良く、利用者の多いネットワークに近い場所に設置すれば、全体のネットワーク負荷を軽減することができる。

【0048】

#### 【発明の効果】

インターネットを用いた情報発信システムにおいて、情報登録を容易にし、負荷を軽減し、不正な情報の登録や改ざんの検知が容易となり、改ざんされた場合でも元情報への訂正も容易にできる為、システムの構成および管理の手間と費用を大幅に改善できる。

#### 【図面の簡単な説明】

##### 【図1】

従来の技術を示すシステム構成図。

##### 【図2】

他の従来の技術を示す構成図。

##### 【図3】

本発明の実施の形態を示す概略システム構成図。

##### 【図4】

図3に対し、ファイアウォールを隠して防護性を良くしたシステム構成図。

##### 【図5】

図4に対し、スイッチを利用して更に防護性を良くし負荷分散性能も良くした

システム構成図。

【図 6】

図 5 のシステムを装置として実装した場合の例を示す図。

【図 7】

電子署名の評価による配信制御を示す図。

【図 8】

コンペアチェックの構成例を示す図。

【図 9】

即時更新機能の構成例を示す図。

【図 1 0】

ファイアウォールの構成例を示す図。

【図 1 1】

ネームサーバの構成例を示す図。

【図 1 2】

電子署名を用いた情報発信制御を示すフローチャート。

【図 1 3】

複数の電子署名を用いた情報発信制御を示すフローチャート。

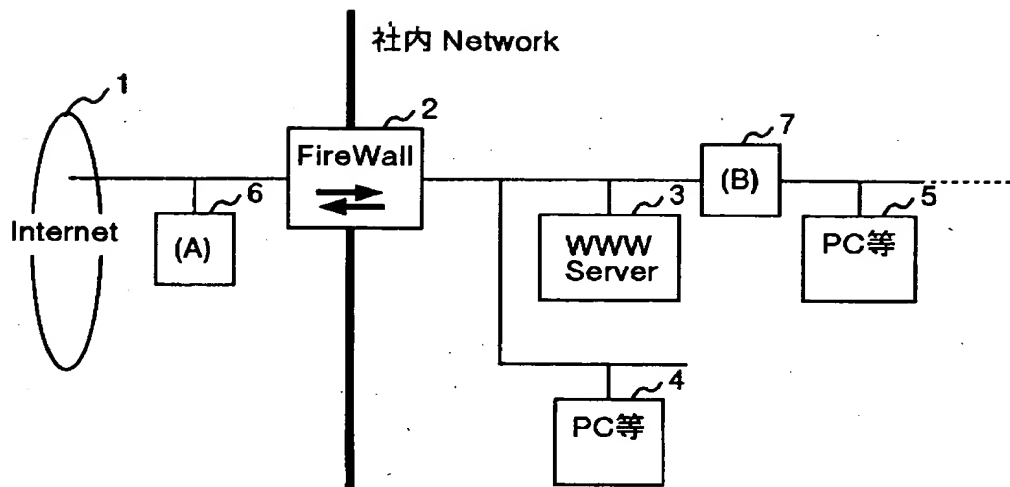
【符号の説明】

- 1 インタネット
- 2 ファイアウォール（防火壁）
- 3 WWWサーバ
- 4 登録情報作成システム
- 5 ルータで保護された登録情報作成システム
- 8 レプリカ
- 9 ネームサーバ
- 1 0 負荷分散スイッチ
- 1 1 WWWセキュリティ装置

【書類名】 図面

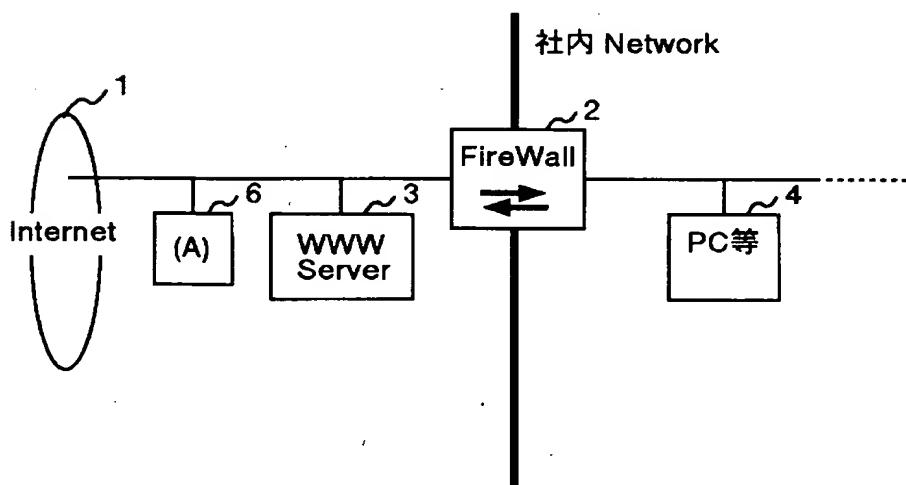
【図 1】

図 1



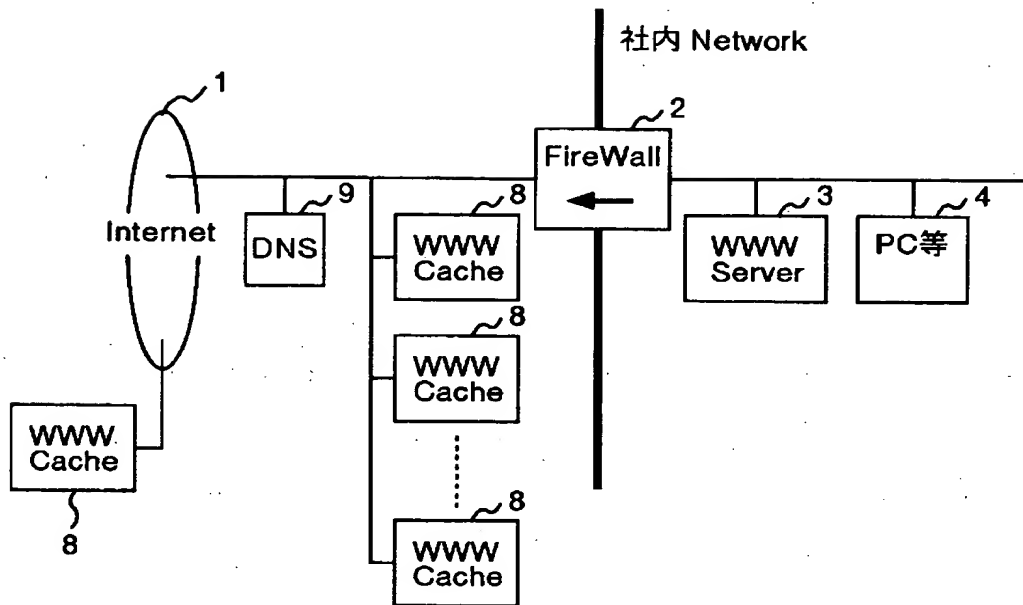
【図 2】

図 2



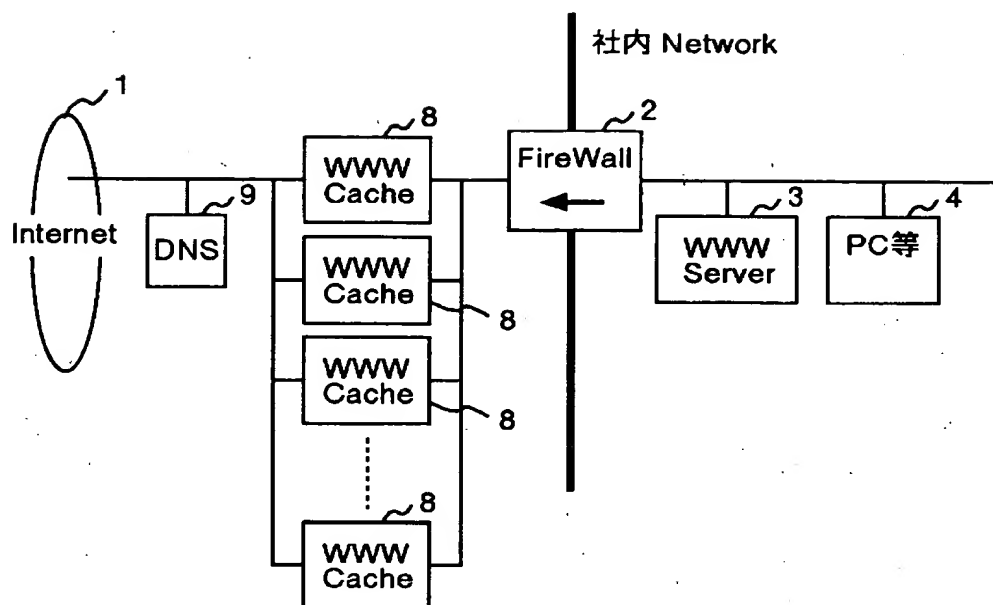
【図 3】

図 3



【図 4】

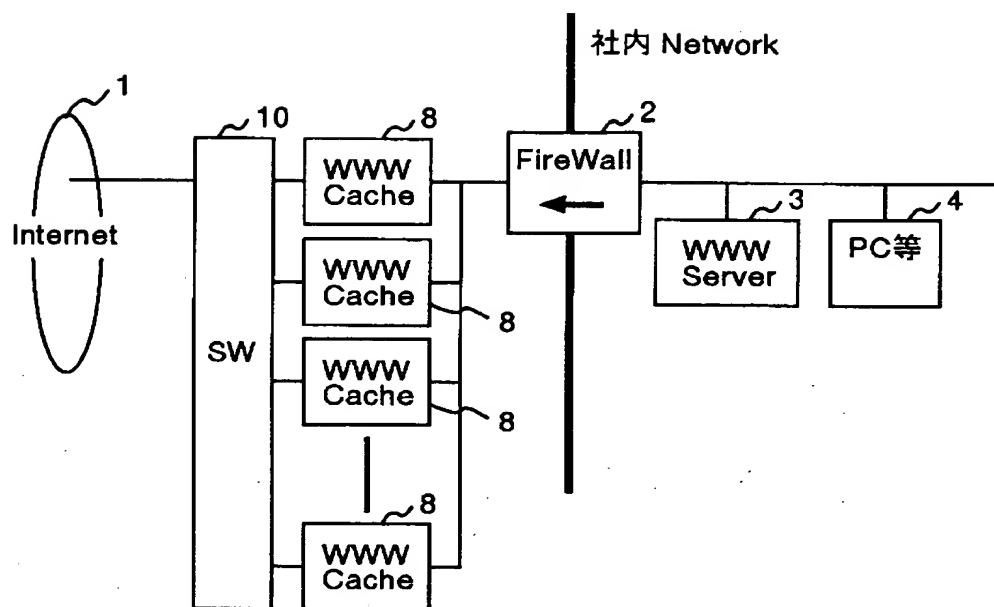
図 4





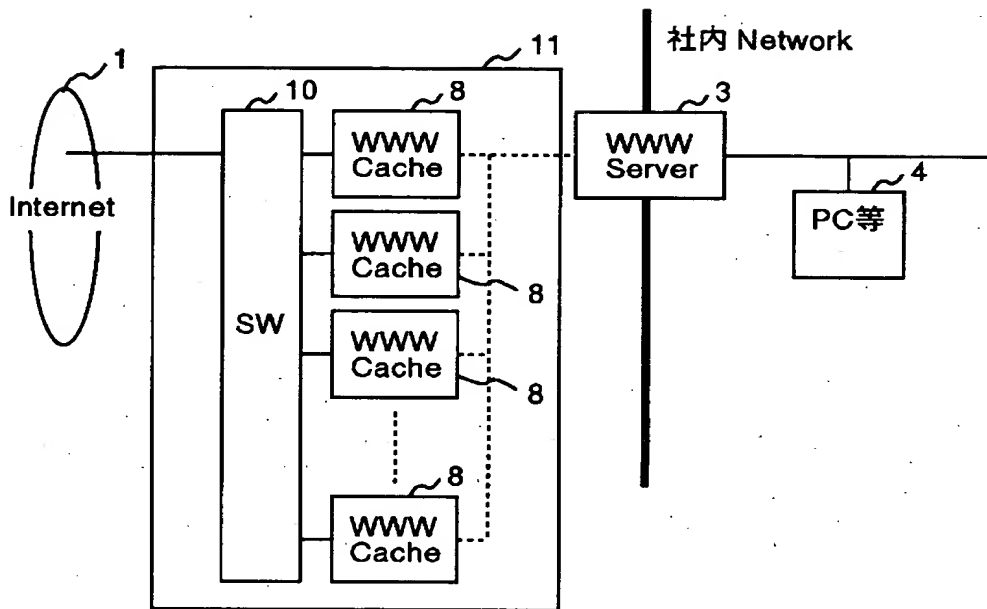
【図 5】

図 5



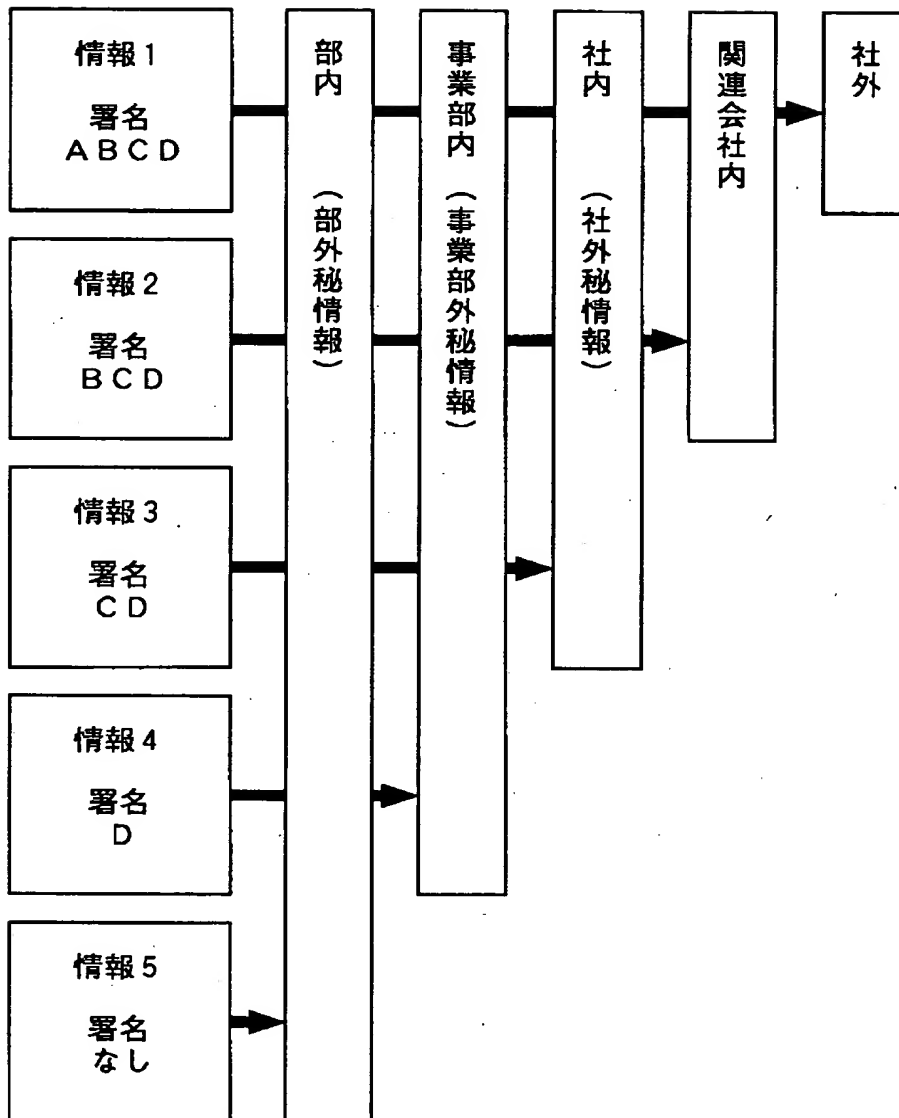
【図 6】

図 6



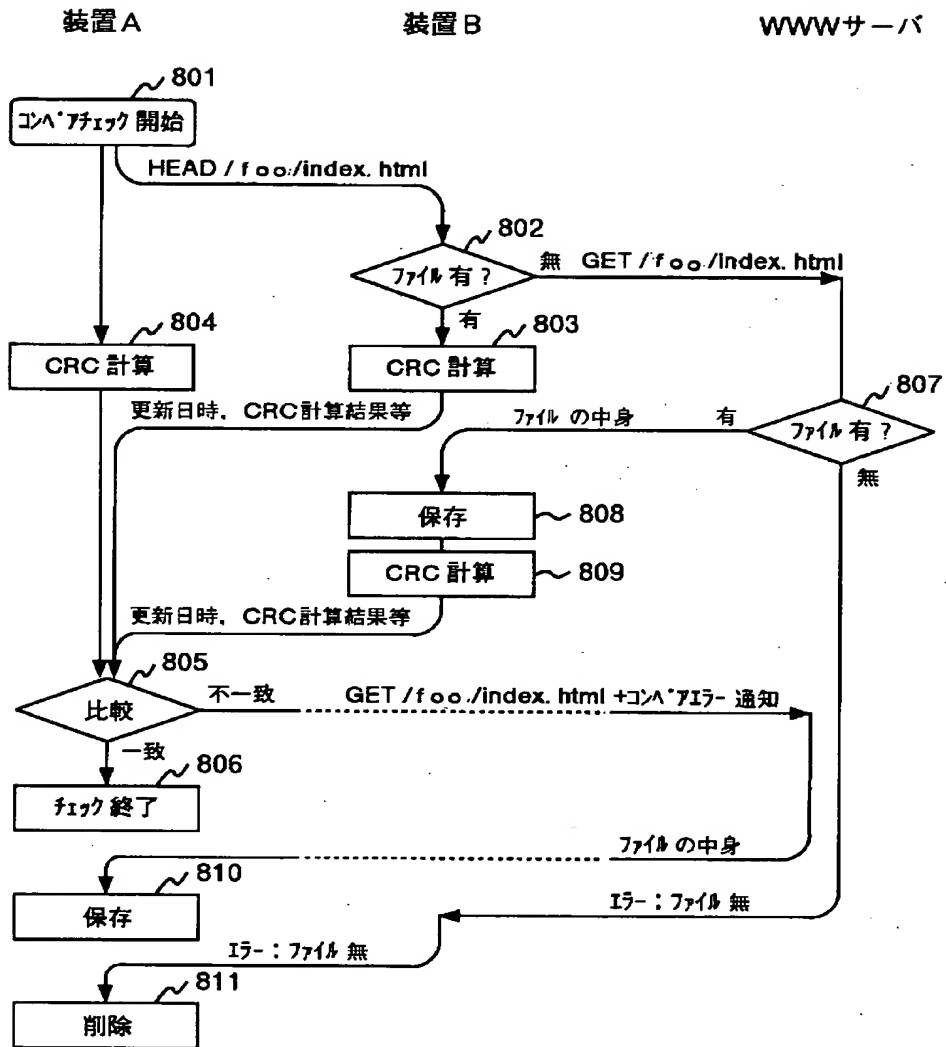
【図 7】

図 7



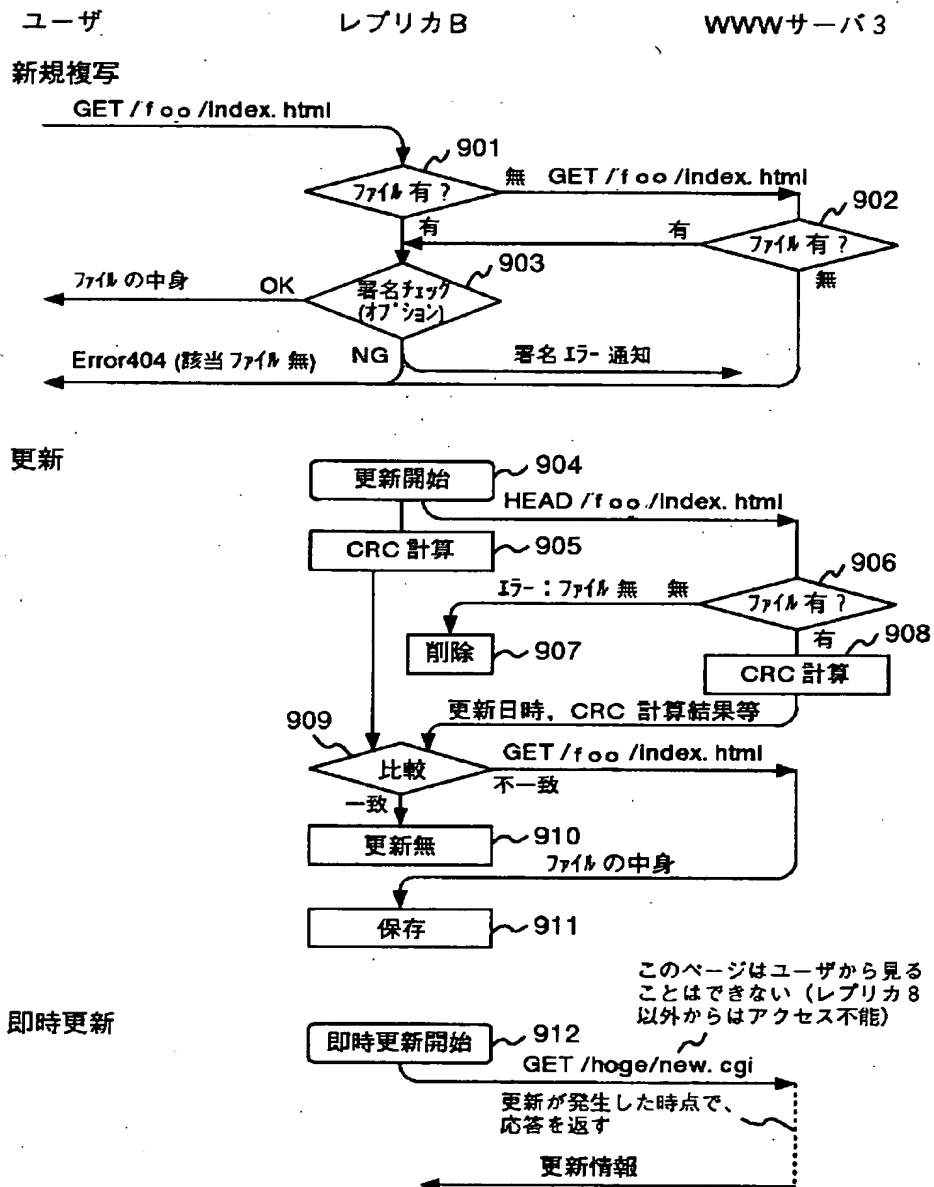
【図 8】

図 8



【図 9】

図 9



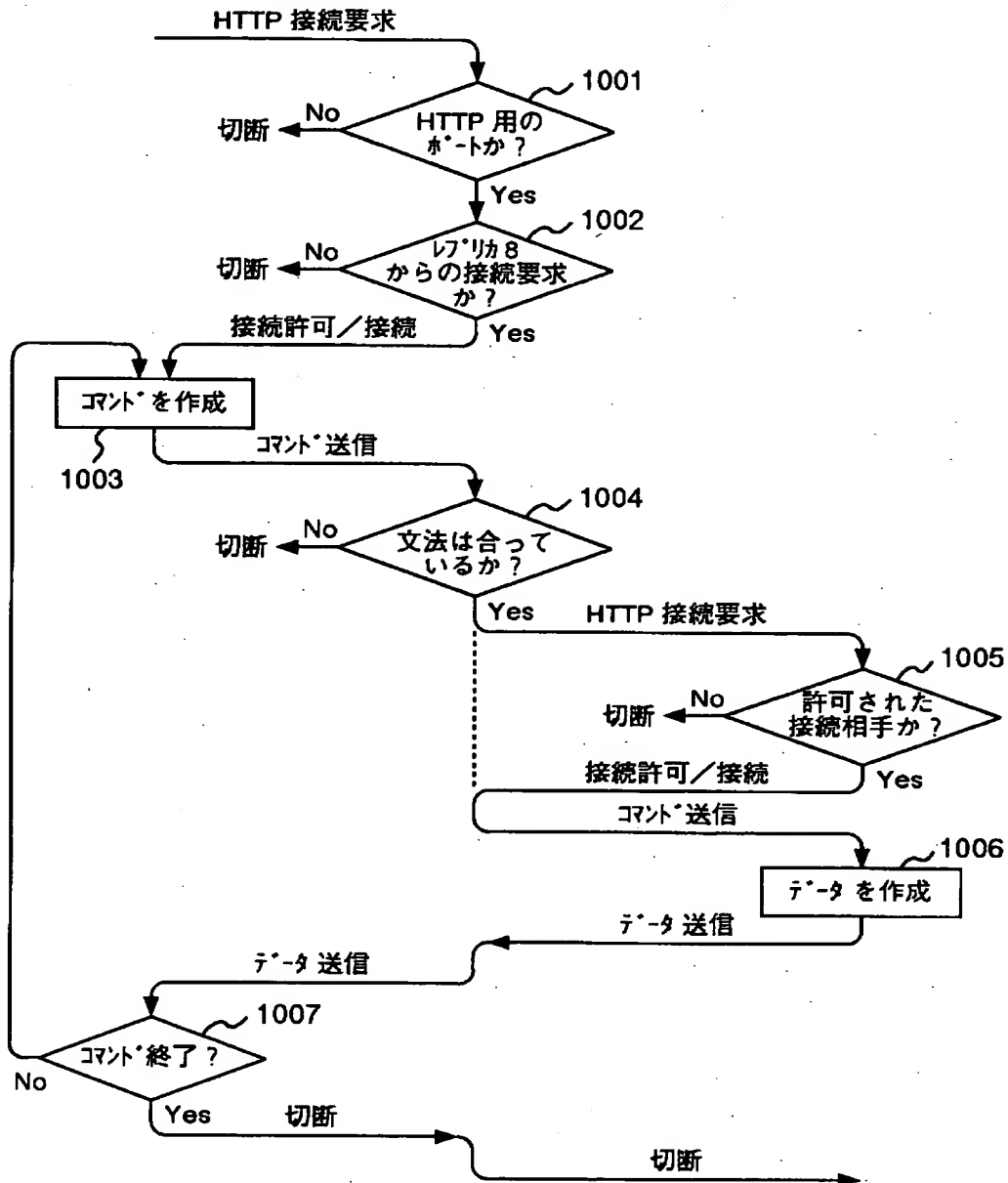
【図 10】

図 10

レプリカ 8

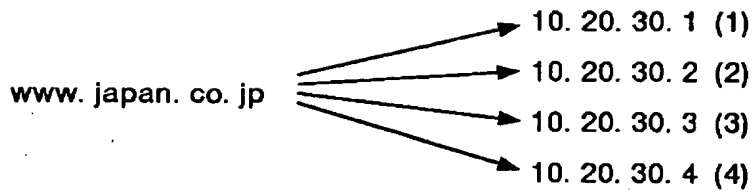
ファイアウォール 2

WWWサーバ 3



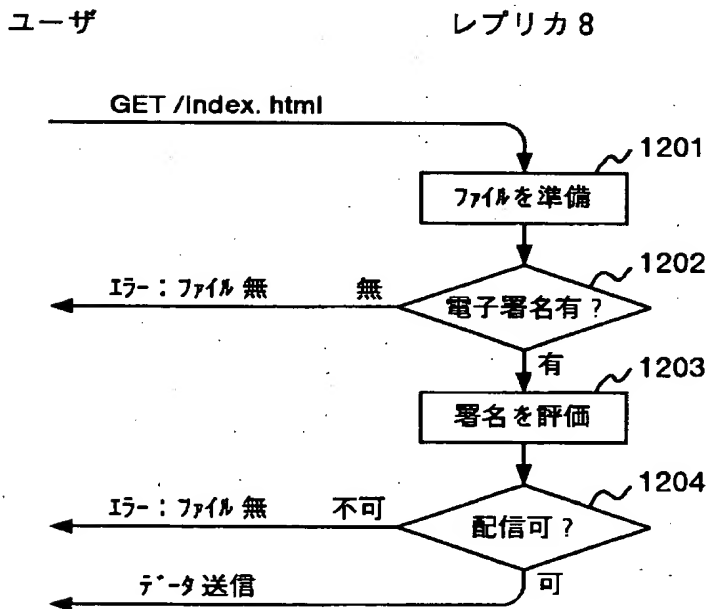
【図 1 1】

図 1 1



【図 1 2】

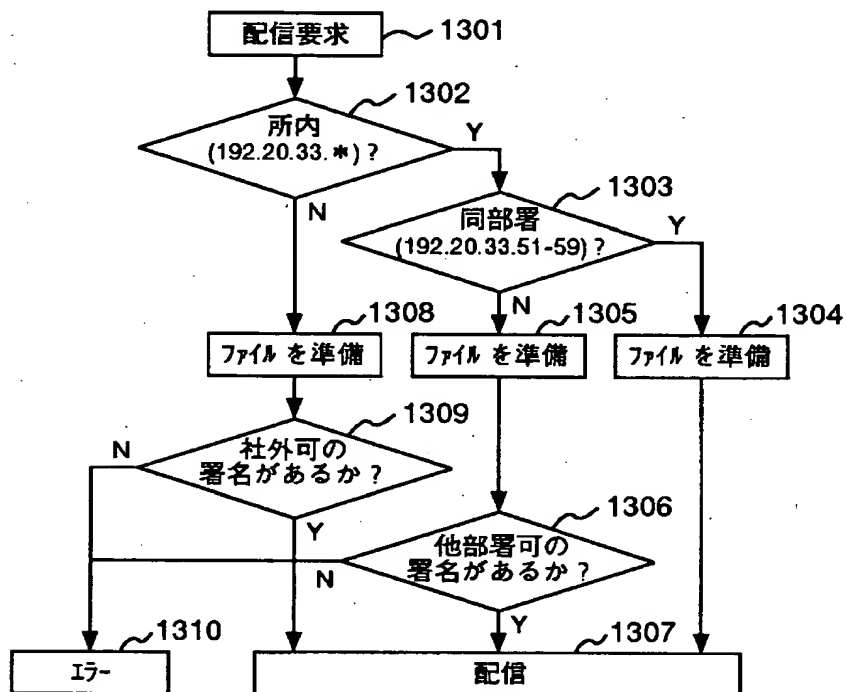
図 1 2



【図 13】

図 13

ユーザ A (社外)	ユーザ B (社内他部署)	ユーザ C (社内同部署)
IP:172.16.199.201	IP:192.20.33.44	IP:192.20.33.56





【書類名】 要約書

【要約】

【課題】 インタネットに接続されていて不特定多数の利用者に情報を発信するコンピュータシステムにおいて、内外からの不正な侵入や改ざんからシステム全体を防護する簡便な方法がなかった。

【解決手段】 インタネットから見える装置は情報発信機器の複製のみとし、複製を複数設置することにより互いに比較させ改ざんを検出する。複製は電子署名の検査を実施し、不正であった場合は改ざんが発生したと見なし情報発信機器 3 から本来あるべき情報を再複製することもできる。情報発信機器はファイアウォール 2 により保護されているので、情報登録は容易に行うことができる。

【選択図】 図 3

特2000-316200

出願人履歴情報

識別番号 [000005108]

1. 変更年月日 1990年 8月31日

[変更理由] 新規登録

住 所 東京都千代田区神田駿河台4丁目6番地

氏 名 株式会社日立製作所